

JUN. 12. 2006 4:14PM  
TO: USPTO

ZILKA-KOTAB, PC

NO. 3202 P. 1

**ZILKA-KOTAB**  
PC  
ZILKA, KOTAB & FEECE™

**RECEIVED**  
CENTRAL FAX CENTER

**JUN 12 2006**

100 PARK CENTER PLAZA, SUITE 300  
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573  
FAX (408) 971-4660

**FAX COVER SHEET**

<b>Date:</b> June 12, 2006	<b>Phone Number</b>	<b>Fax Number</b>
<b>To:</b> Board of Patent Appeals	(571) 273-8300	
<b>From:</b> Kevin J. Zilka		

**Docket No.:** NAIIP345/01.239.01

**App. No: 10/068,280**

**Total Number of Pages Being Transmitted, Including Cover Sheet: 34**

**Message:**

Please deliver to the Board of Patent Appeals.

Thank you,  
Kevin J. Zilka

☐ Original to follow Via Regular Mail ☒ Original will Not be Sent ☐ Original will follow Via Overnight Courier

\*\*\*\*\*  
The information contained in this facsimile message is attorney privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copy of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by telephone (if long distance, please call collect) and return the original message to us at the above address via the U.S. Postal Service. Thank you.  
\*\*\*\*\*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER  
ANY OTHER DIFFICULTY, PLEASE PHONE Erica  
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

June 12, 2006

RECEIVED  
CENTRAL FAX CENTER

JUN 12 2006

Practitioner's Docket No. NAI1P345/01.239.01

PATENT

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Mark J. McArdle et al.

Application No.: 10/068,280

Group No.: 2135

Filed: 02/04/2002

Examiner: Ha, L.

For: INTRUSION PREVENTION FOR ACTIVE NETWORKED APPLICATIONS

Mail Stop Appeal Briefs - Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF  
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on April 10, 2006.
2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

06/13/2006 TL0111 00000024 501351 10068280  
01 FC:1402 500.00 DA

## CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10\*

(When using Express Mail, the Express Mail label number is mandatory;  
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

## MAILING

\_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)

\_ with sufficient postage as first class mail.

37 C.F.R. § 1.10\*

\_ as "Express Mail Post Office to Addressee"

Mailing Label No. \_\_\_\_\_ (mandatory)

## TRANSMISSION

\_ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

Date:

6/12/2006

Signature

Erica L. Farlow

(type or print name of person certifying)

\* Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(j). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

Transmittal of Appeal Brief--page 1 of 2

**RECEIVED  
CENTRAL FAX CENTER****JUN 12 2006****3. FEE FOR FILING APPEAL BRIEF**

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity \$500.00

**Appeal Brief fee due \$500.00**

**4. EXTENSION OF TERM**

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant(s) believe that no Extension of Time is required; however, if it is determined that such an extension is required, Applicant(s) hereby petition that such an extension be granted

**5. TOTAL FEE DUE**

The total fee due is:

Appeal brief fee \$500.00

Extension fee (if any) \$0.00

**TOTAL FEE DUE \$500.00**

**6. FEE PAYMENT**

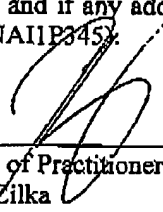
Authorization is hereby made to charge the amount of \$500.00 to Deposit Account No. 50-1351 (Order No. NAI1P345).

A duplicate of this transmittal is attached.

**7. FEE DEFICIENCY**

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P345).

Reg. No.: 41,429  
Tel. No.: 408-971-2573  
Customer No.: 28875

  
\_\_\_\_\_  
Signature of Practitioner  
Kevin J. Zilka  
Zilka-Kotab, PC  
P.O. Box 721120  
San Jose, CA 95172-1120  
USA

Transmittal of Appeal Brief--page 2 of 2

JUN 12 2006

## PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: )  
McArdle et al. ) Group Art Unit: 2135  
Application No. 10/068,280 ) Examiner: Ha, Leynna A.  
Filed: 02/04/2002 ) Date: 06/12/2006  
For: INTRUSION PREVENTION FOR )  
ACTIVE NETWORKED APPLICATIONS )  
\_\_\_\_\_ )

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**ATTENTION: Board of Patent Appeals and Interferences****APPEAL BRIEF (37 C.F.R. § 41.37)**

This brief is in furtherance of the Notice of Appeal, filed in this case on 04/10/2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

- I REAL PARTY IN INTEREST
- II RELATED APPEALS AND INTERFERENCES
- III STATUS OF CLAIMS
- IV STATUS OF AMENDMENTS
- V SUMMARY OF CLAIMED SUBJECT MATTER
- VI ISSUES
- VII ARGUMENTS

- 2 -

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY APPELLANT IN THE APPEAL

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

- 3 -

**I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))**

The real party in interest in this appeal is McAfee, Inc.

- 4 -

## **II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))**

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, below is a list of such appeals, interferences, or related judicial proceedings.

No such pending appeals, interferences, or related judicial proceedings exist.

A Related Proceedings Appendix is appended hereto.

- 5 -

**III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))**

**A. TOTAL NUMBER OF CLAIMS IN APPLICATION**

Claims in the application are: 1-51

**B. STATUS OF ALL THE CLAIMS IN APPLICATION**

1. Claims withdrawn from consideration: None
2. Claims pending: 1-51
3. Claims allowed: None
4. Claims rejected: 1-51
5. Claims cancelled: None

**C. CLAIMS ON APPEAL**

The claims on appeal are: 1-51

See additional status information in the Appendix of Claims.



- 6 -

**IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))**

As to the status of any amendment filed subsequent to final rejection, there is no amendment after final.

- 7 -

**V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))**

With respect to a summary of Claims 1, 15, 29, and 43 and as shown in Figures 1-3B, a computerized method, a computer-readable medium, a system, and an apparatus are set forth. First, current active networked applications are determined (e.g. see item 205 of Fig. 2, etc.). Next, a set of intrusion rules are filtered (e.g. see item 103 of Fig. 1, etc.) to create a subset of intrusion rules corresponding to the active networked application (e.g. see specification, page 5, lines 19-22). The subset of the intrusion rules correspond to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application (e.g. see item 105 of Fig. 1, etc.). Further, network traffic is evaluated using the subset of intrusion rules (e.g. see item 215 of Fig. 2, etc.). The subset of the intrusion rules corresponding to the active networked application are used for the evaluation, for reducing a required amount of processing resources (e.g. see specification, page 6, lines 16-19, etc.).

- 8 -

**VI ISSUES (37 C.F.R. § 41.37(c)(1)(vi))**

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claim 51 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Issue # 2: The Examiner has rejected Claims 1-12, 14-26, 28-40, 42-48, 50-51 under 35 U.S.C. 103(a) as being unpatentable over Freund (U.S. Patent No. 5,987,611) in view of Kaler et al. (U.S. Patent No. 6,671,829).

Issue # 3: The Examiner has rejected Claims 13, 27, 41, 49 under 35 U.S.C. 103(a) as being unpatentable over Freund in view of Kaler et al. in view of Official Notice.

- 9 -

**VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))**

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

**Issue # 1:**

The Examiner has rejected Claim 51 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The Examiner has specifically stated that appellant's claimed technique "wherein the heuristic rule includes information associated with an active networked application making a new connection never previously made" is not supported in the specification. Appellant respectfully points out page 5, lines 1-8 of the specification, which clearly states that "a heuristic rule may describe an attack that is based on unusual behavior, e.g. an application suddenly making a new, previously unseen connection" and that "[t]he system 100 applies a filter 103 based on the active networked applications." Thus, appellant's claim language is clearly supported by the specification.

In the Advisory Action mailed 03/15/2006, the Examiner argued that "[t]he proposed claim stated "a new connection never previously made" is interpreted as a brand new connection that never made or completed attempts before.' In addition, the Examiner argued that 'the specification states "a new, previously unseen connection", is not the same as a new connection "never" previously made.' Further, the Examiner argued that "[t]he claimed previously unseen connection of the specification is interpreted as a connection that was previously undetected or unknown of but does not mean a connection that was never made." Appellant respectfully disagrees with the Examiner's interpretation and respectfully asserts that page 5, lines 1-4 of the specification teaches that "a heuristic rule may describe an attack that is based on unusual behavior, e.g. an application suddenly making a new, previously unseen connection" (emphasis added). Appellant asserts that since the connection is new, it supports appellant's claimed "new connection never previously made," since a new connection would not previously have been seen.

- 10 -

Issue # 2:

The Examiner has rejected Claims 1-12, 14-26, 28-40, 42-48, 50-51 under 35 U.S.C. 103(a) as being unpatentable over Freund (U.S. Patent No. 5,987,611) in view of Kaler et al. (U.S. Patent No. 6,671,829). Appellant respectfully disagrees with such rejection.

*Group #1: Claims 1, 7-12, 14-15, 21-26, 28-29, 35-40, 42-43, 47, and 50*

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the *prima facie* case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner argues that it would have been obvious to combine the teaching of the subset of intrusion rules in Freund with the teaching of filter reduction to extract only the information of interest as taught by Kaler because this reduces the performance impact of monitoring. To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Freund and Kaler references, especially in view of the vast evidence to the contrary.

For example, Freund relates to regulating access and maintaining security of individual computer systems and local area networks connected to larger open networks, while Kaler relates to analyzing the performance of a data processing system. To simply glean features from a security system, such as that of Freund, and combine the same with the *non-analogous art* of a performance analyzer, such as that of Kaler, would simply be improper. In particular, security systems actively protect computer systems, while performance analyzers merely collect data associated with a computer system for performance analysis. "In order to rely on a reference as a

- 11 -

basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992). In view of the vastly different types of problems a security system addresses as opposed to a performance analyzer, the Examiner's proposed combination is inappropriate.

In the Advisory Action mailed 03/15/2006, the Examiner argued that "[t]he security system of Freund and performance analyzer of Kaler both monitors and filters data and therefore both comprises security prevention." In addition, the Examiner argues that "[t]o analyze the performance is clearly to attempt to protect the system, otherwise there is not a need to analyze its traffic or activities." However, the abstract of Kaler discloses "a distributed data processing system...[that] provide[s] a system user with tools for analyzing an application running thereon" in which "[i]nformation about the flow and performance of the application can be specified, captured, and analyzed, without modifying it or degrading its performance or data security characteristics, even if it is distributed across multiple machines" (Kaler, Abstract - emphasis added). Clearly, Kaler's disclosure that flow and performance information can be specified, captured, and analyzed, without degrading its data security characteristics *teaches away* from any sort of security system, contrary to the Examiner's assertion that Kaler "comprises security prevention." Thus, for the reasons argued above, the Examiner's proposed combination of Kaler's performance analyzer with Freund's security system is inappropriate.

Appellant also respectfully asserts that the third element of the *prima facie* case of obviousness has also not been met by the references relied on by the Examiner. Specifically, with respect to each of the independent claims, the Examiner has relied on the following excerpts from Freund to make a prior art showing of appellant's claimed "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (see the same or similar, but not necessarily identical language in each of the independent claims).

"...the system can track files being created and changed by any process in order to match TCP/IP activities with corresponding file activities." (Col. 4, lines 65-67)

- 12 -

"...which specifies rules which govern Internet access by the client computers including the particular client computer;  
c) Transmitting a filtered subset of the rules to the particular client computer." (Col. 5, lines 39-43)

Appellant respectfully asserts that the only rules in such excerpts relate to "rules which govern Internet access by the client computers." Clearly, rules that govern Internet access do not meet appellant's claimed "rules corresponding to the active networked application" (emphasis added).

Furthermore, simply because Freund teaches that a "system can track files created and changed by any process" does not inherently mean that there are rules corresponding to an active networked application, in the manner claimed by appellant.

Still yet, such excerpts do not even mention any sort of filtering, let alone "filtering a set of intrusion rules to create a subset of intrusion rules," as appellant specifically claims (emphasis added). In fact, appellant notes that the only subset of rules disclosed in Freund relate to "rules filtered for a given user" (see Claim 12 in Freund), and not to appellant's claimed "subset of intrusion rules corresponding to the active networked application" (emphasis added).

In the Advisory Action mailed 03/15/2006, in addressing appellant's claimed "filtering a set of intrusion rules to create a subset of intrusion rules," the Examiner argued that "Kaler was brought forth to explain the filtering creating subset rules process" and "that a filter is a way in which a user can specify [what is] to be monitored in the system under examination (col. 22, lines 2-7)." However, a system user specifying what is monitored in a system fails to even suggest "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (emphasis added), as claimed by appellant.

Further, in the Advisory Action mailed 03/15/2006, in addressing appellant's claimed "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application," the Examiner argued that "Freund does have the claimed filtering rules corresponding to the active networked application (col. 10, lines 17-67)." Additionally, the Examiner argued that "Freund discusses monitoring and filtering work that is responsible for intercepting process loading and unloading (col. 4, lines 5-33 and col. 5, lines 55-62)."

- 13 -

After carefully reviewing the cited references, it is clear that Freund merely discloses that "[t]he client-based filter application, which in a preferred embodiment performs all of the monitoring, logging, and filtering work, is responsible for intercepting process loading and unloading" (emphasis added). Freund further discloses that the "Client Monitor compares application properties (version, executable name, and the like) with database of application allowed to access the Internet" (emphasis added). However, the client based filter application and the Client Monitor comparing application properties with a database of applications allowed to access the internet simply fails to meet "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (emphasis added), as claimed by appellant. The referenced excerpts from Freund simply fail to even suggest any rule filtering "corresponding to the active networked application," as claimed by appellant.

In addition, the Examiner argued that "Freund does have the claimed filtering rules corresponding to the active networked application (col. 10, lines 17-67)." Further, with respect to each of the independent claims, the Examiner has relied on the following excerpts from Freund to make a prior art showing of appellant's claimed technique "where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application" (see the same or similar, but not necessarily identical language in each of the independent claims).

"e) Determining whether the request for Internet access would violate any of the rules transmitted to the particular client computer, and  
f) If the request for Internet access violates any of the rules transmitted to the particular client computer, denying the request for Internet access.

II. Using Application Properties to Determine Legitimate Internet Traffic

a) Application attempts to access Internet;  
b) Client Monitor compares application properties (version, executable name, and the like) with database of application allowed to access the Internet and checks what kind of activity the application is allowed to do (mail, browsing, and the like)." (Col. 5, lines 46-59-emphasis added)

"(1) The system should preferably be capable of restricting access to the Internet (or other Wide Area Network) to certain approved applications or/and application versions.  
(2) The system should preferably support centrally-maintained access rules (e.g., defining basic access rights), but at the same time allow individual workgroup managers or even individual users to set rules for their area of responsibility, if so desired by the organization." (Col. 8, lines 45-52)



- 14 -

Appellant respectfully asserts that such excerpts only relate to accessing the Internet, including rules associated with applications that are allowed to access the Internet (see emphasized excerpt above). Clearly, only teaching rules regarding accessing the Internet does not meet appellant's specific claim language, namely a "subset of the intrusion rules corresponding to the active networked application [that] are capable of being used for evaluating intrusions that target the corresponding active networked application" (emphasis added), as claimed.

In the Advisory Action mailed 03/15/2006, in addressing appellant's claimed "subset of the intrusion rules corresponding to the active networked application," the Examiner argued that "[t]he claimed set of intrusion rules is merely interpreted as more than one intrusion rules where Freund does teach more than one intrusion rules and subset rules for the client computer (col. 5, lines 35-62)." Specifically, Freund discloses "[i]nstalling ... a supervisor process, which specifies rules which govern Internet access by the client computers including the particular client computer" and "[t]ransmitting a filtered subset of the rules to the particular client computer" (emphasis added). However, merely specifying rules governing Internet access and transmitting a filtered subset of access rules fails to disclose a technique "where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application" (emphasis added), as claimed by appellant.

Further, in the Advisory Action mailed 03/15/2006, in addressing appellant's claimed "subset of the intrusion rules ... [which] are capable of being used for evaluating intrusions that target the corresponding active networked application," the Examiner argued that "[m]onitoring the application of the computer being used is to access the internet where there involves rules and subset rules to regulate access on a per application basis (col. 10)." The Examiner continued, arguing that "[t]hese filtering rules and subset rules, which includes monitoring a given active application, total time particular applications access the Internet, and limiting the number of (approved) applications are secure measures for evaluating the active networked applications for intrusions."

- 15 -

Appellant respectively asserts that such excerpts from Freund merely teach that '[a] given application itself can be examined for determining whether it is "active" by determining whether the application receives "focus" and/or receives user input' (Col. 10, lines 40-43). In addition, Freund teaches that "the Internet access monitoring system of the present invention can track Internet access on a per application basis—that is, access broken down by the application or applications used for the access" (Col. 10, lines 47-50). However, monitoring the total time the user is browsing the Internet with an application that has the user focus simply fails to meet a technique "where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application" (emphasis added), as claimed by appellant. Appellant asserts that merely disclosing rules for monitoring user Internet usage fails to meet a subset of rules "for evaluating intrusions that target the corresponding active networked application" (emphasis added), as claimed by appellant.

Still yet, with respect to each of the independent claims, the Examiner has relied on the following excerpts et al. from Freund and Kaler to make a prior art showing of appellant's claimed technique "wherein the subset of the intrusion rules corresponding to the active networked application are used for the evaluation for reducing a required amount of processing resources."

"If a process uses FTP to download a file, for example, the system will match that activity to a file being saved by the same process by checking file name and size. If a match is found, a log entry is generated. This allows the immediate application of internal or external virus checkers." (Freund: Col. 13, lines 59-65)

"Filter reduction is used to narrow the scope of the filter to extract only the information of interest and hence reduce the performance impact of monitoring." (Kaler: Col. 4, lines 57-61)

First, appellant respectfully asserts that the excerpt in Freund relied on by the Examiner does not even suggest any sort of "subset of the intrusion rules," as the Examiner contends (emphasis added), but instead only teaches matching activity to a file. Thus, since Freund does not disclose a subset in the context claimed by appellant, Freund cannot teach, even in combination with Kaler, a subset that is "used for the evaluation for reducing a required amount of processing resources." Furthermore, appellant notes that, when read in context, Kaler's filter reduction only relates to a user that specifies which items to filter such that events are collected only for the

- 16 -

specified items (see Kaler, Col. 37, line 47- Col. 38, line 5). Thus, Kaler does not teach a subset of intrusion rules, as claimed by appellant, but instead only teaches a filter that collects events for specified items.

Since at least the first and third elements of the *prima facie* case of obviousness has not been met, as noted above, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

*Group #2: Claims 2, 16, 30, and 44*

With respect to Claim 2 et al., the Examiner has relied on Col. 4, lines 51-62 in Freund to make a prior art showing of appellant's claimed "detecting when the active networked application becomes inactive; and re-filtering the set of intrusion rules." Appellant respectfully asserts that the only mention of an application in such excerpt merely relates to a "system [that] can monitor TCP/IP activities on a...per application basis." Freund simply fails to even suggest a situation where an "active networked application becomes inactive" (emphasis added), and especially does not teach that, when such occurs, "the set of intrusion rules [are re-filtered]," as claimed by appellant.

*Group #3: Claims 3, 4, 17, 18, 31, and 32*

With respect to Claims 3 and 4 et al., the Examiner has relied on Col. 13, lines 20-22 in Freund to make a prior art showing of appellant's claimed technique "wherein the detecting comprises: monitoring network connection terminations" (Claim 3 et al.) and "wherein the detecting comprises: monitoring application terminations" (Claim 4 et al.). Appellant respectfully asserts that such excerpt from Freund only discloses that "if a rule is violated...[then] Internet access [is denied]." Clearly, denying internet access in the case that a rule is violated does not even suggest any sort of monitoring, let alone specifically "monitoring network connection terminations" and/or "monitoring application terminations," as claimed by appellant.

*Group #4: Claims 5, 6, 19, 20, 33, 34, 45, and 46*

- 17 -

With respect to Claim 5 et al., the Examiner has relied on Col. 13, lines 50-56 and Col. 26, lines 55-58 in Freund to make a prior art showing of appellant's claimed "detecting when no networked application is active; and suspending the evaluating of network traffic until a networked application is active." Appellant respectfully asserts that such excerpts only relate to "prescribed remedial action for any violated rule" such that "the communication is...terminated." Clearly, terminating a communication upon detection of a rule violation, as in Freund, does not even remotely relate to appellant's claim language, namely "detecting when no networked application is active," let alone where "the evaluating of network traffic [is suspended] until a networked application is active" (emphasis added).

*Group #5: Claim 48*

With respect to Claim 48, the Examiner has relied on Col. 11, line 56-Col. 12, line 17 and Col. 13, lines 13-22 in Freund to make a prior art showing of appellant's claimed technique "wherein the intrusion rules include information selected from the group consisting of a targeted active networked application, a specific hostile payload, a network port, and a protocol." Appellant respectfully asserts that Col. 11, line 56-Col. 12, line 17 does not relate to intrusion rules, as claimed by appellant, but instead only relates to the protocol the Internet uses. In addition, Col. 13, lines 13-22 only discloses that the rules can specify "to whom the rule should apply...start date and expiration date of a rule; time of day when the rules should be applied...whether the rule is 'disclosed' to the user or workgroup...whether a rule can be overwritten...and what should happen if a rule is violated." Clearly, such information associated with the rules as taught in Freund only relate to the application of the rules, and not to the substance of the rules including "a targeted active networked application, a specific hostile payload, a network port, and a protocol," as specifically claimed by appellant.

*Group #6: Claim 51*

With respect to Claim 51, the Examiner has relied on Col. 10, lines 31-44; Col. 30, lines 13-15; Col. 13, lines 34-42; and Col. 5, lines 39-43 in Freund to make a prior art showing of appellant's claimed technique "wherein the heuristic rule includes information associated with an active networked application making a new connection never previously made." Appellant respectfully

- 18 -

asserts that such excerpts only disclose that a "given application itself can be examined for determining whether it is 'active' by determining whether the application receives 'focus' and/or receives user input," "maintain[ing] a list of active Applications," "each client process can be checked for various characteristics," and "rules which govern Internet access." First, appellant respectfully asserts that such excerpts do not even suggest any sort of heuristic rule, as claimed by appellant. Second, only determining which applications are actively used by a user, as in Freund, clearly does not meet any sort of "information associated with an active networked application making a new connection never previously made," as specifically claimed by appellant (emphasis added).

Again, since at least the first and third elements of the *prima facie* case of obviousness has not been met, as noted above, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Issue # 3:

The Examiner has rejected Claims 13, 27, 41, 49 under 35 U.S.C. 103(a) as being unpatentable over Freund in view of Kaler et al. in view of Official Notice. Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued above with respect to Issue #2, Group #1.

Appellant again respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

- 19 -

**VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))**

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computerized method comprising:  
determining an active networked application;  
filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application, where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application; and  
evaluating network traffic using the subset of intrusion rules;  
wherein the subset of the intrusion rules corresponding to the active networked application are used for the evaluation for reducing a required amount of processing resources.
2. (Original) The computerized method of claim 1 further comprising:  
detecting when the active networked application becomes inactive; and  
re-filtering the set of intrusion rules.
3. (Original) The computerized method of claim 2, wherein the detecting comprises:  
monitoring network connection terminations.
4. (Original) The computerized method of claim 2, wherein the detecting comprises:  
monitoring application terminations.
5. (Original) The computerized method of claim 1 further comprising:  
detecting when no networked application is active; and  
suspending the evaluating of network traffic until a networked application is active.
6. (Original) The computerized method of claim 1, wherein the subset of rules further corresponds to an operating system and further comprising:  
continuing the evaluating of network traffic if no networked application is active.

- 20 -

7. (Original) The computerized method of claim 1, wherein the determining comprises:  
detecting when a network connection for an active application is initiated.
8. (Original) The computerized method of claim 1, wherein the filtering comprises:  
marking an intrusion rule corresponding to the active networked application.
9. (Original) The computerized method of claim 1, wherein the filtering comprises:  
extracting the subset of rules into an optimized set of rules.
10. (Original) The computerized method of claim 1, wherein the evaluating comprises:  
analyzing network traffic on a port specified in the subset of rules.
11. (Original) The computerized method of claim 1, wherein the evaluating comprises:  
analyzing network traffic for a protocol specified in the subset of rules.
12. (Original) The computerized method of claim 1, wherein the evaluating comprises:  
discarding network traffic that satisfies at least one of the subset of rules; and  
reporting an intrusion attempt.
13. (Original) The computerized method of claim 1, wherein the set of intrusion rules  
comprises signatures of known attacks.
14. (Original) The computerized method of claim 1, wherein the set of intrusion rules  
comprises heuristic rules.
15. (Previously Presented) A computer-readable medium having executable instructions to  
cause a computer to perform a method comprising:  
determining an active networked application;  
filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the  
active networked application, where the subset of the intrusion rules corresponding to the active

- 21 -

networked application are capable of being used for evaluating intrusions that target the corresponding active networked application; and

evaluating network traffic using the subset of intrusion rules;

wherein the subset of the intrusion rules corresponding to the active networked application are used for the evaluation for reducing a required amount of processing resources.

16. (Original) The computer-readable medium of claim 15, wherein the method further comprises:

detecting when the active networked application becomes inactive; and  
re-filtering the set of intrusion rules.

17. (Original) The computer-readable medium of claim 16, wherein the detecting comprises:  
monitoring network connection terminations.

18. (Original) The computer-readable medium of claim 16, wherein the detecting comprises:  
monitoring application terminations.

19. (Original) The computer-readable medium of claim 15, wherein the method further comprises:

detecting when no networked application is active; and  
suspending the evaluating of network traffic until a network application is active.

20. (Original) The computer-readable medium of claim 15, wherein the subset of rules further corresponds to an operating system and the method further comprises:

continuing the evaluating of network traffic if no networked application is active.

21. (Original) The computer-readable medium of claim 15, wherein the determining comprises:

detecting when an active application initiates a network connection.

22. (Original) The computer-readable medium of claim 15, wherein the filtering comprises:

marking an intrusion rule corresponding to the active networked application.



- 22 -

23. (Original) The computer-readable medium of claim 15, wherein the filtering comprises:  
extracting the subset of rules into an optimized set of rules.
24. (Original) The computer-readable medium of claim 15, wherein the evaluating comprises:  
analyzing network traffic on a port specified in the subset of rules.
25. (Original) The computer-readable medium of claim 15, wherein the evaluating comprises:  
analyzing network traffic for a protocol specified in the subset of rules.
26. (Original) The computer-readable medium of claim 15, wherein the evaluating comprises:  
discarding network traffic that satisfies at least one of the subset of rules; and  
reporting an intrusion attempt.
27. (Original) The computer-readable medium of claim 15, wherein the set of intrusion rules comprises signatures of known attacks.
28. (Original) The computer-readable medium of claim 15, wherein the set of intrusion rules comprises heuristic rules.
29. (Previously Presented) A system comprising:  
a processor coupled to a memory through a bus; and  
an intrusion prevention process executed from the memory by the processor to cause the processor to determine an active networked application, to filter a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application, where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application, and to evaluate network traffic using the subset of intrusion rules;

- 23 -

wherein the subset of the intrusion rules corresponding to the active networked application are used for the evaluation for reducing a required amount of processing resources.

30. (Original) The system of claim 29, wherein the intrusion prevention process further causes the processor to detect when the active networked application becomes inactive, and to re-filter the set of intrusion rules.

31. (Original) The system of claim 30, wherein the intrusion prevention process further causes the processor to monitor network connection terminations in detecting when the active networked application becomes inactive.

32. (Original) The system of claim 30, wherein the intrusion prevention process further causes the processor to monitor application terminations in detecting when the active networked application becomes inactive.

33. (Original) The system of claim 29, wherein the intrusion prevention process further causes the processor to detect when no networked application is active, and to suspend evaluating network traffic until a network application is active.

34. (Original) The system of claim 29, wherein the intrusion prevention process further causes the processor to further filter the intrusion rules based on an operating system and to continue evaluating network traffic if no networked application is active.

35. (Original) The system of claim 29, wherein the intrusion prevention process further causes the processor to detect when an active application initiates a network connection in determining an active networked application.

36. (Original) The system of claim 29, wherein the intrusion prevention process further causes the processor to mark an intrusion rule corresponding to the active networked application in filtering the set of intrusion rules.

- 24 -

37. (Original) The system of claim 29, wherein the intrusion prevention process further causes the processor to extract the subset of rules into an optimized set of rules in filtering the set of intrusion rules.

38. (Original) The system of claim 29, wherein the intrusion prevention process further causes the processor to analyze network traffic on a port specified in the subset of rules in evaluating the network traffic.

39. (Original) The system of claim 29, wherein the intrusion prevention process further causes the processor to analyze network traffic for a protocol specified in the subset of rules in evaluating the network traffic.

40. (Original) The system of claim 29, wherein the intrusion prevention process further causes the processor to discard network traffic that satisfies at least one of the subset of rules, and to report an intrusion attempt in evaluating the network traffic.

41. (Original) The system of claim 29, wherein the set of intrusion rules comprises signatures of known attacks.

42. (Original) The system of claim 29, wherein the set of intrusion rules comprises heuristic rules.

43. (Previously Presented) An apparatus comprising:

means for determining when an active application becomes an active networked application;

means for filtering coupled to the means for determining to create a subset of intrusion rules corresponding to the active networked application from a set of intrusion rules, where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application; and

means for evaluating coupled to the means for filtering to evaluate network traffic using the subset of intrusion rules;

- 25 -

wherein the subset of the intrusion rules corresponding to the active networked application are used for the evaluation for reducing a required amount of processing resources.

44. (Original) The apparatus of claim 43, wherein the means for determining further detects when the active networked application becomes inactive and the means for filtering further re-filters the set of intrusion rules when the active networked application becomes inactive.

45. (Original) The apparatus of claim 43, wherein the means for determining further detects when no networked application is active and the means for evaluating further suspends the evaluation of network traffic until the means for determining determines a networked application is active.

46. (Original) The apparatus of claim 43, wherein the means for filtering further filters the intrusion rules corresponding to an operating system and the means for evaluating continues the evaluation of network traffic when the means for determining determines no networked application is active.

47. (Original) The apparatus of claim 43, wherein the means for evaluating comprises:  
means for discarding network traffic that satisfies at least one of the subset of rules; and  
means for reporting an intrusion attempt.

48. (Previously Presented) The computerized method of claim 1, wherein the intrusion rules include information selected from the group consisting of a targeted active networked application, a specific hostile payload, a network port, and a protocol.

49. (Previously Presented) The computerized method of claim 1, wherein the intrusion rules include an attack signature.

50. (Previously Presented) The computerized method of claim 1, wherein at least one of the intrusion rules is a heuristic rule.

- 26 -

51. (Previously Presented) The computerized method of claim 50, wherein the heuristic rule includes information associated with an active networked application making a new connection never previously made

- 27 -

**IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY APPELLANT IN THE  
APPEAL (37 C.F.R. § 41.37(c)(1)(ix))**

There is no such evidence.

- 28 -

**X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))**

N/A

- 29 -

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAIIP345).

Respectfully submitted,

By: 

Kevin J. Zilka

Reg. No. 41,429

Date: 6/12/06

Zilka-Kotab, P.C.

P.O. Box 721120

San Jose, California 95172-1120

Telephone: (408) 971-2573

Facsimile: (408) 971-4660